



Feuilleton

Mein Leben im Griff der Ermittlungsbehörden

Marko Rogge

Ausspähen von Daten in Tateinheit mit versuchter Computersabotage (§§ 202a, 303b I Nr.1, 303a, 22, 23I, 52 StGB). Ein persönlicher Tatsachenbericht von Marko Rogge.

Einleitung und Tatverdacht

Am 06.10.2006 soll nach Angaben des Sicherheitschefs einer großen Firma in Oberfranken versucht worden sein, einen Zugriff auf das Computersystem der Firma zu erhalten. Es soll versucht worden sein, einen Zugriff auf den Webserver zu erlangen, um dann im weiteren durch die Firewall zu gelangen. Hierbei sollen Passwortabfragen generiert worden sein, so das Protokoll der Kriminalpolizei. Nach den Aussagen des verantwortlichen Sicherheitschefs der angegriffenen Firma ist jedoch die Firewall nicht überwunden worden.

Aufgrund dessen wurde am 17.10 beantragt, einen Durchsuchungsbeschluss zu erwirken, um die Hardware zu beschlagnahmen. Am 27.10 wurde entsprechend nach §§ 94, 98 StPO eine Beschlagnahme angeordnet, sofern Computer nebst Peripherie zzgl. Unterlagen und Aufzeichnungen nicht freiwillig herausgegeben werden.

Im Durchsuchungsbeschluss wird dann sinngemäß begründet:

Es bestehe der Verdacht, dass ich durch unterschiedlichste Abfragen versucht haben soll, das Betriebssystem des Webserver der betroffenen Firma herauszufinden. Ebenso soll durch mich versucht worden sein, einen so genannten Buffer-Overflow auf dem Webserver auszuführen. Ein Buffer-Overflow ist der Begriff für einen Angriff, bei dem versucht wird, den Speicher der Anwendung so anzugreifen, dass diese Anwendung den Dienst versagt, und der Angreifer dadurch höhere Rechte erlangen kann. (http://de.wikipedia.org/wiki/Buffer_Overflow).

Es wurde weiterhin angeführt, dass ich ebenfalls verdächtigt werde, im Anschluss mehrere Datenbankabfragen auf der Webseite durchgeführt zu haben. Dabei soll ich nach Angaben der Sicherheitsexperten der betroffenen Firma in den Besitz der internen IP-Adresse des Webserver gelangt sein.

Im Protokoll der Kriminalpolizei ist nachzulesen, dass der Administrator/Verantwortliche im IDS (Intrusion Detection System) festgestellt hat, dass im Logfile des IDS die

interne IP als die angegriffene IP angezeigt wurde. Daraus schlussfolgerte der Verantwortliche selbständig, dass es nur möglich sei, durch Datenausspähung in den Besitz dieser internen IP-Adresse zu gelangen. Da es sich hierbei um eine nicht-öffentliche IP Adresse handelt, wurde Anzeige erstattet. Die zu dem Zeitpunkt mir zugeordnete IP Adresse wurde in den Logfiles der betroffenen Firma gefunden, und so wurde diese IP Adresse als Grundlage zur Anzeige gebracht, und die Ermittlungen wurden aufgenommen.

Ich werde im Verlauf dieses Berichtes noch darauf eingehen, wie ich herausgefunden habe, dass hierbei kein Ausspähen von Daten vorlag.

Die Ermittlungen und die Hausdurchsuchung

Die erste Hausdurchsuchung war für den 09.11.2006 angesetzt und sollte gleich morgens durchgeführt werden. Nach Angaben der Kriminalpolizei hat niemand im Haus die Tür geöffnet, und man ist unverrichteter Dinge wieder gegangen. Es wurde auch festgehalten, dass ich nicht zu Hause war und somit auch nicht Kenntnis von der bevorstehenden Hausdurchsuchung haben konnte. Das entspricht auch den Tatsachen.

Am 24.11.2006 erfolgte dann der 2. Versuch, die Hausdurchsuchung durchzuführen. Diese erfolgte in der Zeit von 08:00-09:00 Uhr, und es wurden diverse Gegenstände beschlagnahmt:

Ein Computer, eine Firewall, eine externe Festplatte sowie ein WLAN Access Point (AP).

Welchen Hintergrund die Beschlagnahme der Firewall und des WLAN AP hatte, ist mir bis heute unverständlich. Mir wurde jedoch dazu erklärt, dass man die Logfiles auswerten wolle.

Es sollte hier erwähnt werden, dass auch darüber diskutiert wurde, mein Mobiltelefon zu beschlagnahmen, da es ja über WLAN verfüge. Die 3 Ermittler und eine weitere Person als Zeuge haben sich dann aber dazu entschlossen, es dabei zu belassen, und ich sollte es nur nicht nutzen, solange die Beschlagnahme dauerte.

Es war mir in dem Zusammenhang untersagt, meine eigenen Gegenstände der EDV zu berühren.

Man erklärte, dass der Computer mit dem Linux System nach München geschickt werden müsse, und

die externe Festplatte in Bayreuth untersucht werde. Was mit der Firewall und dem WLAN AP geschehen ist, und welche Untersuchungen vorgenommen wurden, ist bis heute nicht bekannt.

Hier möchte ich anmerken, dass ich mich mit der Hausdurchsuchung nicht bereit erklärt habe und auch nicht mit der Sichtung meiner persönlichen Papiere. Die Herausgabe der EDV Anlage musste dennoch erfolgen, und so sind die Ermittler zur Tat geschritten. Vorsichtig und umsichtig wurde gefragt, wie man es am besten machte, da man nichts zerstören wollte. Währenddessen hat ein weiterer Ermittler sich an meinen privaten Unterlagen, die auf dem Küchentisch lagen, zu schaffen gemacht. Dies war nicht Gegenstand der Untersuchung oder Beschlagnahme, und dies hatte ich zudem ausdrücklich verweigert. Dennoch ist es geschehen, gegen meinen eigenen Willen.

Die Untersuchung der Hardware, Ergebnisse und Schlussfolgerungen daraus

Auf der externen Festplatte habe man Schadsoftware gefunden, so das Protokoll. Es wurde über den Zeitstempel der externen Festplatte festgestellt, dass diese am Angriffstag nicht in Betrieb war. Seltsam, dass man trotzdem die Daten untersuchte, vermutlich um dennoch Spuren finden zu können. Die Festplatte wurde mir dann schnellstens wieder ausgehändigt, da die ermittelnde Staatsanwaltschaft diese nicht als Tatwerkzeug ansah.

Am 30.3.2007 kam das Ergebnis der Untersuchung des Computers, der nun aus München eingetroffen war.

Satte 21 Stunden habe der Sachverständige des LKA damit zugebracht, mein Fedora Linux entsprechend auf Angriffspuren zu untersuchen. In den Logfiles des Systems wurden keine Spuren gefunden, die den Computer mit einer Straftat in Zusammenhang bringen. Man fand unter anderem einen Unterordner *exploits* im */home/* Verzeichnis und einige Dokumente, die auf **.doc* enden. Aus den Quellinformationen und der Endung **.doc* schlussfolgerte der Sachverständige, dass es sich hierbei um Microsoft Word Dateien handeln müsse.

Der Sachverständige ging davon aus, dass mir demnach weitere Rechner mit Windows installiert zur Verfügung stehen mussten, da es für Linux keine Software gäbe, die ein solches Format öffnen und erstellen könne. Sicherlich muss man sich fragen, ob der Sachverständige schon etwas von OpenOffice gehört hat, und dass man damit auch unter WORD erstellte Dokumente weiter bearbeiten kann.

Über den Autor

Marko Rogge, selbst Betroffener dieses Falls ist Sicherheitsberater und anerkannter Autor diverser Publikationen, und veröffentlicht regelmäßig Artikel in Hakin9 und anderen Fachzeitschriften. Er berät Unternehmen seit Jahren in Hinblick auf IT-Sicherheit und hilft so mit, dass Unternehmen vor böswilligen Hackerangriffen geschützt sind.

Mehr: <http://www.marko-rogge.de>

Warum man hier in Richtung eines Windows System ermittelte, ist mir nicht schlüssig, da mit einem Windows Computer ein Angriff dieser Art nicht durchführbar gewesen wäre.

Es wurde ebenfalls bei der Untersuchung des Computers festgestellt, dass es grundsätzlich möglich sei, eine IP Adresse zu fälschen. Auf meinem Computer wurde keine dafür notwendige Spyware gefunden.

Welchen Sinn eine Spyware auf meinem eigenen Computer machen sollte, ist für mich mehr als unklar.

Ein Angreifer würde außerdem sicherlich keine Spyware verwenden, um eine IP Adresse zu fälschen, sondern würde vielmehr auf eine Spoofing Methode zurück greifen.

Man benötigt einen einfachen IP Scanner, um in einem IP Range (Adressbereich) herauszufinden, wer online ist und wer nicht. Jede beliebige IP Adresse, die als online registriert wird, eignet sich somit zum Fälschen.

Als ich während meiner Vernehmung anführte, dass man bedenken solle, dass jemand Fremdes über meinen vorhandenen *WLAN Access Point (AP)* Zugriff erhalten und meine IP genutzt haben könnte, ging man nicht näher darauf ein. Denn auch diese Möglichkeit ist technisch realisierbar. Angreifbar ist man auch als Sicherheitsexperte – genauso wie jeder andere.

In der Ausführung der Ermittlungsbeamten heißt es im Anschluss an die Vernehmung wieder ganz anders.

Plötzlich taucht der Begriff einer *Crackersoftware* auf, die jemand verwendet haben müsse, um unmittelbar in meiner Wohnungsnähe in den AP einzudringen. Es erscheint den Beamten der Kriminalpolizei merkwürdig, dass ich mir nicht mehr sicher war, wie ich meinen AP gesichert hatte. Schlichtweg wusste ich zum Zeitpunkt meiner Vernehmung einfach nicht mehr, welche Verschlüsselung ich eingesetzt hatte und ob diese auch aktiviert war. Der AP war schon lange Zeit vor der Beschlagnahme nicht mehr mit dem Netzwerk verbunden. Dennoch ist er beschlagnahmt worden, und er sollte untersucht werden. Die ermittelnden Beamten hätten bei der Untersuchung sehen müssen, welche Verschlüsselung im Einsatz war.

Im Zuge der Ermittlungen durchleuchtete man mein komplettes Leben und das Umfeld, in dem ich zu diesem Zeitpunkt lebte. Nächtliche Besuche vor der Wohnung sind protokolliert worden. Was genau die Ermittler nachts vor meinem Wohnhaus ermitteln wollten, ist mir unklar; zu den Gründen wurde nichts protokolliert.

Es sollte ein Zusammenhang hergestellt werden zu der Frage, ob ich versucht haben soll, durch einen solchen Angriff Geld von der Firma zu erpressen oder einen Auftrag zu erhalten. Die Ermittler gingen aufgrund der Gesamtumstände davon aus, dass ich selbst für den Angriff auf das Netzwerk der betroffenen Firma verantwortlich sei. Ebenfalls wurde angemerkt, dass ich mir durch die Aufdeckung von Sicherheitslücken neue Aufträge verschaffen wollte.

Man ist nicht weiter darauf eingegangen, als ich mich dazu äußerte, dass ich ja wohl in dem Fall in irgendeiner Form mit der Firma in Verbindung getreten

wäre. Das war jedoch nicht der Fall. In Bezug dazu habe ich ausgesagt, dass ich durch Surfen auf der Webseite der jetzt betroffenen Firma 4 Jahre zuvor zufällig eine Schwachstelle entdeckt hatte. Diese Schwachstelle hatte ich umgehend einer zuständigen Stelle der Firma gemeldet, um Schaden von der Firma abzuwenden. Auch zu dem damaligen Zeitpunkt hatte ich in dem Zusammenhang keine meiner Dienstleistungen der Firma angeboten. Ein Danke für den damaligen Hinweis ist von der Firma bis heute nicht an mich ausgesprochen worden.

Der Ausgang und das Ende

Nach mehrmaligem Lesen der Ermittlungsakten ist mir recht spät erst aufgefallen, dass hier ein nicht unerheblicher Fehler gemacht wurde. Die Verantwortlichen der betroffenen Firma hatten ja festgestellt, dass die interne IP Adresse vermeintlich dem Angreifer in die Hände gelangt sei. Das entsprach aber nicht den Tatsachen, da man im internen Logfile der Firma auch rein logisch nur die internen IP Adressen sehen kann. Diese Gegebenheit führte in der Folge dazu, dass die internen IP Adressen als angegriffene (und ausgespähte) angesehen wurden.

Da meine IP Adresse als Angreifer-IP Adresse ebenfalls im Logfile stand, wurde Anzeige zunächst gegen Unbekannt und nach der Zuordnung zu meinem Anschluss gegen mich erstattet. Nachdem mein Rechtsanwalt Carsten Hoenig und ich nun in der Lage waren, den Vorwurf des Ausspähens von Daten eindeutig zu entkräften, blieb noch der ausgeführte aber nicht erfolgreiche Buffer Overflow im Raum stehen. Auch diesen soll ich ausgeführt haben.

Den Buffer Overflow sowie auch den Angriff auf die interne IP Adresse habe ich nicht durchgeführt und war auch nie daran interessiert, solche Angriffe auszuführen. Ich möchte hier anmerken, dass man mich dafür bezahlt, dass ich solche Angriffe auf Firmen durchführe, um unter echten Bedingungen die Sicherheit und Stabilität der Netzwerke und/oder Server zu prüfen. Einen Angriff, wie er mir vorgeworfen wurde, würde ich niemals ohne einen zuvor erteilten Auftrag ausführen.

Es folgte eine deutliche Argumentation meines Rechtsanwaltes, die aufzeigte, dass nichts auf eine Täterschaft hindeutete. In meinem Arbeitsumfeld, aus dem der Computer und die anderen Geräte beschlagnahmt wurden, sind keine Spuren oder Hinweise gefunden worden. Allein die Tatsache, im Besitz von so genannten Exploits oder anderer Schadsoftware zu sein, reicht nicht aus. Auch die ermittelnden Beamten der Kripo sind zu dem Schluss gekommen, dass es sich hierbei schließlich um Arbeitswerkzeug meiner Branche handele. Einer weiteren Sachverständigenuntersuchung wurde nicht entsprochen, und diese schien nicht notwendig.

Am 30.08.2007 war es dann soweit:

Das Ermittlungsverfahren wurde nach der Strafprozessordnung §170 Abs.2 am 30.8.2007 von der Staatsanwaltschaft eingestellt. ●